IJTRET "Voice of Innovative Minds"
doi.org.10.54473/IJTRET.2023.7602
International Journal of Trendy Research in Engineering and Technology
Volume 7 Issue 6 December 2023
ISSN No.2582-0958

# MEDICAL IMAGE ENCRYPTION USING DNA SEQUENCING AND AFFINE TRANSFORM

Soniya Sarathe[1] and Chetan Gupta[2] Dr.Ritu Shrivastava[3]
[1]M. Tech. Scholar, [2]Asst.Professor, [3]Prof. & Head, Department of Computer Science & Engineering,
Sagar Institute of Research & Technology, Bhopal, India
Received 05 December 2023 Received in revised form 15 December 2023 Accepted 18 December 2023
Available online 20 December 2023

**ABSTRACT**

The present study introduces a new approach to encrypting medical images. The available encryption algorithms are good for text data. They may not be suitable for multimedia data, especially for sensitive medical image data. Indeed, the pixels of natural and biological images exhibit a significant correlation with their adjacent pixels. As a result of this robust correlation, it is feasible to predict the value of any given pixel based on the values of its neighboring pixels. The utilization of DNA encoding and Affine transform is employed in this research for medical image application. DNA-based encryption offers several benefits such as extensive data storage capacity, parallel processing abilities, and enhanced security through biological complexity. The presented algorithm was tested on a variety of biomedical data. The assessment metrics indicate that the suggested scheme for image encryption exhibits favorable statistical characteristics. It is seen from evaluation metrics that the proposed image encryption scheme provides a proficient and reliable method for promptly encrypting and transmitting biomedical images in the field of telemedicine.

**Keywords:** Image Encryption, Medical image, Affine transform, DNA encoding, Image security.

## I. INTRODUCTION

Because of advancements in computer network technology, exchanging information between users of personal computers is now becoming much less time consuming and more comfortable. Meanwhile, it provides opportunity for hackers to launch attacks on the network. As a result, the problem of communication security has become more significant in the context of multimedia communications. Image data, including medical photos, photographs from the military, images from electronic publication, and fingerprint images from identification systems, need to be kept private and secret at all times. The current healthcare business relies heavily on the practice of medical image analysis, which in turn has a significant influence on the modern world [1]. When it comes to the diagnosis of biological imaging, automated computer-aided systems are quite helpful since they are quick, accurate, and efficient. Through the use of remote healthcare systems, both patients and medical professionals are able to execute their duties from their respective places [2][3]. In addition, within a certain length of time, a physician in a different nation or in any other remote place may be contacted to provide an expert opinion about a patient who is being treated by that physician. Digital images need to be sent via an open network for remote healthcare systems to function [4]. However, the transmission of biomedical images is coupled with many potential vulnerabilities in terms of security. The images must be protected from any type of unauthorized access to maintain the patients' right to privacy. In addition, the information included within the biological pictures has to be effectively kept so that it cannot be modified in any way. The manipulation of data may, in many circumstances, have major effects [5]. As a result, the procedures and algorithms affecting sensitive data security are of the utmost significance, and they are among the topics that are receiving the most attention from researchers working in this field.

## II. RELATED WORK

The utilization of edge maps was proposed by Cao et al. [6] as a means of implementing an encryption method. The approach comprises of three distinct constituents, namely a bit-plane decomposer, a random sequence generator, and a permutation phase. The selection of an appropriate technique for bit-plane decomposition is adaptable, and the proposed algorithm can be combined with numerous permutation methods. The presented technique for securing diverse medical images exhibits a wide key space and high key sensitivity. Li et al. [7] proposed an approach based on a chaotic system comprising the two-dimensional Sine Logistic modulation map (2D-SLMM) and the two-dimensional Henon-Sine map (2D-HSM). The primary encryption technique comprises of three main components, namely zigzag scan scramble, pixel grey value transformation, and dynamic diffusion. The proposed technique for The proposed technique for encrypting and decrypting medical images does not entail any loss of data. The aforementioned approach circumvents the challenges that are associated with low-dimensional chaotic maps characterized by a narrow interval and limited parameters.

Telem et al. [8] introduced the cryptosystem using Affine Transformation and Zigzag Process. The system's operation involves the utilization of both an internal secret key and an external secret key, with the latter being 128 bits in length. They reported that their encryption process lies in the techniques employed for the extraction of an internal key for the application of the zigzag process, the affine transformation, and the substitution-diffusion process. The algorithms were assessed on a diverse range of images encompassing both biomedical and nonmedical domains. Medical image encryption based on DNA and a chaotic map was suggested by Kumari et al. [9]. This approach consists of three phases: the chaotic map generator, DNA complementing, and sequencing of DNA values. The suggested method offers sufficient security and efficient calculation time due to the high degree of confusion, random distribution features, and chaotic approach unpredictability. An approach that makes use of a chaotic map, DNA encoding, and SHA-256 is suggested for medical image security [10]. To ensure that the integrity of the digitalized medical image is maintained, the hash key is first masked in the image's least significant byte once it has been produced using the SHA-256 algorithm. In order to maintain its confidentiality, the picture was encrypted utilising DNA coding methods. The pixels that make up the encoded DNA matrix are jumbled and scattered using Chen's hyper chaotic map.

Arnold chaotic AES-based medical image encryption was proposed by Shalaby et al. [11]. Initially, a Butterworth High Pass Filter was employed to ensure the preservation of medical data while undergoing encryption. Their proposed method has been adapted through the integration of the Arnold chaos technique with the commonly employed AES algorithm. The standard AES key is enhanced by the modification of Arnold's cat map technique, which involves framing and introducing three bits. The encryption methodology under consideration is evaluated in comparison to existing literature. The comparative analysis illustrates that the approach has the capability to enhance the potency of the cryptographic mechanism and the excellence of medical images, while concurrently reducing the total computational expenditure. The hybrid chaos-based medical picture encryption technique was described by Sarosh et al. [12]. The scheme uses multiple chaotic maps, such as Logistic, Chebyshev, and Piecewise, to introduce uncertainty and promote dispersal. In the work, Pseudo-Random sequences are used in the Logistic map to jumble the final picture. The shuffled picture is XOR'd with a key image generated by the piecewise map. At the end, a Chebyshev map iterates and a random sequence is constructed to permute the picture pixels and produce ciphered image. The cryptosystem has been tested on a variety of medical image types and sizes, as well as natural images.

Goje et al. [13] suggested a medical picture encryption technique based on a double chaotic map. The approach uses a 2D chaotic map to describe permutation and a 3D chaotic map to represent diffusion. Encryption techniques make extensive use of the ideas of confusion and diffusion. The authors performed tests and analyzed the data using many metrics (including histogram analysis, correlation, NPCR, UACI, entropy, etc.) to determine whether or not the suggested system was secure.

## III. Proposed methodology

### 3.1 DNA Sequence

Nucleotide is considered as the fundamental building block of biological DNA. The chemical bonding structure of nucleotides results in their categorization into four distinct alphabets. The four nucleotide bases that comprise DNA are commonly referred to as Thymine (T), Guanine (G), Adenine (A), and Cytosine (C) [14]. The linkages are arranged in a structure of a twofold twist due to the presence of the crucial hydrogen. Within the sequence base, a single link is paired with another, such as T and A or C and G, forming a joint structure.

In the binary numeral system, the digit 1 is regarded as the complement of 0. Likewise, the binary sequence 11 is regarded as the complement of 00, and the sequence 10 is regarded as the complement of 01. The nucleotide bases of DNA, namely thymine (T), guanine (G), adenine (A), and cytosine (C), are represented by binary digits 00, 10, 11, and 01, respectively. By utilising this particular concept, a total of 24 distinct encoding samples can be obtained. The complement relation between DNA bases restricts the number of encoding patterns to only eight, which satisfies the complementary base pairing.

### 3.2Affine Transformation

An affine transformation is a type of transformation that maintains co linearity, meaning that all points that are initially situated on a line will remain on a line after the transformation. Additionally, this type of transformation preserves ratios of distances, such that the midpoint of a line segment will remain the midpoint even after the transformation has been applied. The term "affine" denotes a distinctive category of projective transformations that exhibit the property of not inducing any displacement of objects from the affine space onto the plane at infinity, or vice versa.

Consider an affine transformation on the Euclidean plane, which can be described by an equation as follows [15]:

$$w(x,y) = (ax + by + e, cx + dy + f) \quad (1)$$

$$w(x,y) = (x' + y') \quad (2)$$

where
$(x, y)$ - coordinate point,
$(a, b, c, d, f)$ - real numbers,
$(x', y') -$ new coordinate point.

### 3.3Process

To encrypt an image using DNA sequences and an affine transform, you can follow the steps outlined below:

- Image Representation: Convert the image into a numerical representation, such as grayscale intensity.
- DNA Encoding: Map the numerical representation of the image onto a DNA sequence. Assign specific DNA bases (A, T, G, C) to each numerical value or range of values. For example, you can assign a range of intensity values to each DNA base.
- Affine Transform: Apply an affine transformation to the DNA sequence. The affine transform can involve operations like scaling, rotation, shearing, and translation. This step helps scramble the DNA sequence and enhance security.

To decrypt the encrypted image, the following steps are performed:

- Reverse the affine transform to recover the original DNA sequence.
- Perform the inverse DNA mapping to obtain the numerical representation of the image.
- Reconstruct the image from the numerical representation.

By combining DNA encoding and an affine transform with cryptographic techniques, this encryption process adds an extra layer of security to the image data. The complexity of DNA sequences and the mathematical properties of affine transformations contribute to enhanced encryption and protection of sensitive information.

## IV. RESULT AND ANALYSIS

The practicality of the proposed algorithm was tested and verified through the utilization of the MATLAB platform. In order to comprehend the impact of the DNA and affine transformation procedures, Figure 1 displays plain image alongside their respective encrypted and decrypted image.

**Histogram Analysis:** The histograms of the plain and encrypted images utilizing the suggested approach are depicted in Figure 2. The histograms of the encrypted images exhibit uniform distribution. The utilization of the aforementioned method validates its resilience against statistical attacks. The level of security provided by the encryption method is highly robust.

**Correlation Coefficient and Entropy:**
Table 1 displays the correlation coefficients and entropy values of the encrypted images across various medical images. Figure 3 illustrates the arrangement of adjacent pixels, both horizontally, vertically, and diagonally, in both the plain image and its encrypted image.

**PSNR and SSIM:** The evaluation of the Peak Signal-to-Noise Ratio (PSNR) and SSIM (Structural Similarity Index Measure) was conducted on medical test images. The results indicate that the SSIM values were consistently 1, while the PSNR values were infinitely high. These findings are presented in Table 1. The decrypted image and the original image exhibit complete similarity in all instances.

**Comparative Analysis:** Comparison of Correlation coefficient for chest medical image with different literature is illustrated in Table 2.

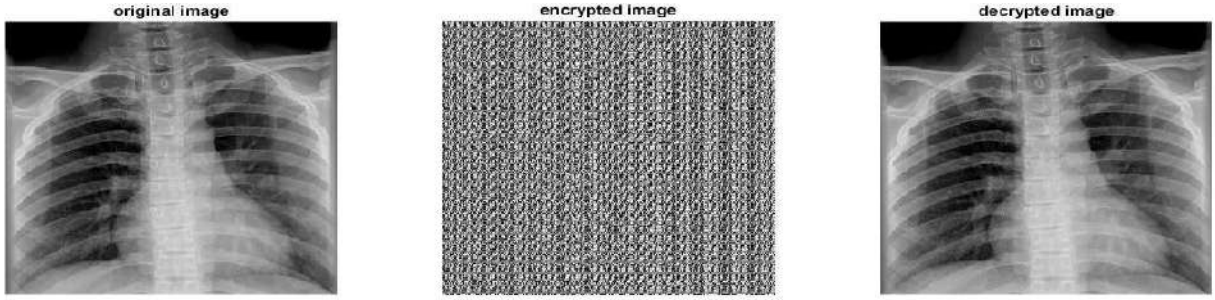


**Fig. 1.** Visual Analysis on Chest image

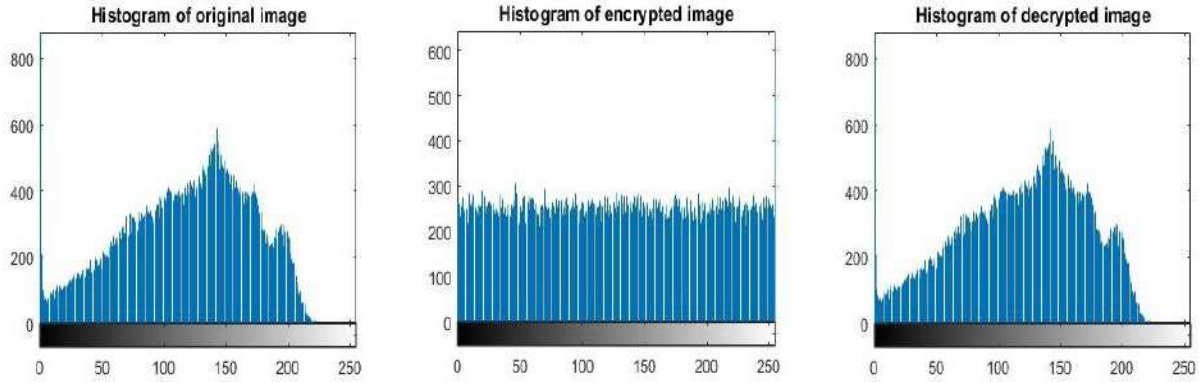


**Fig. 2.** Histogram analysis on chest image

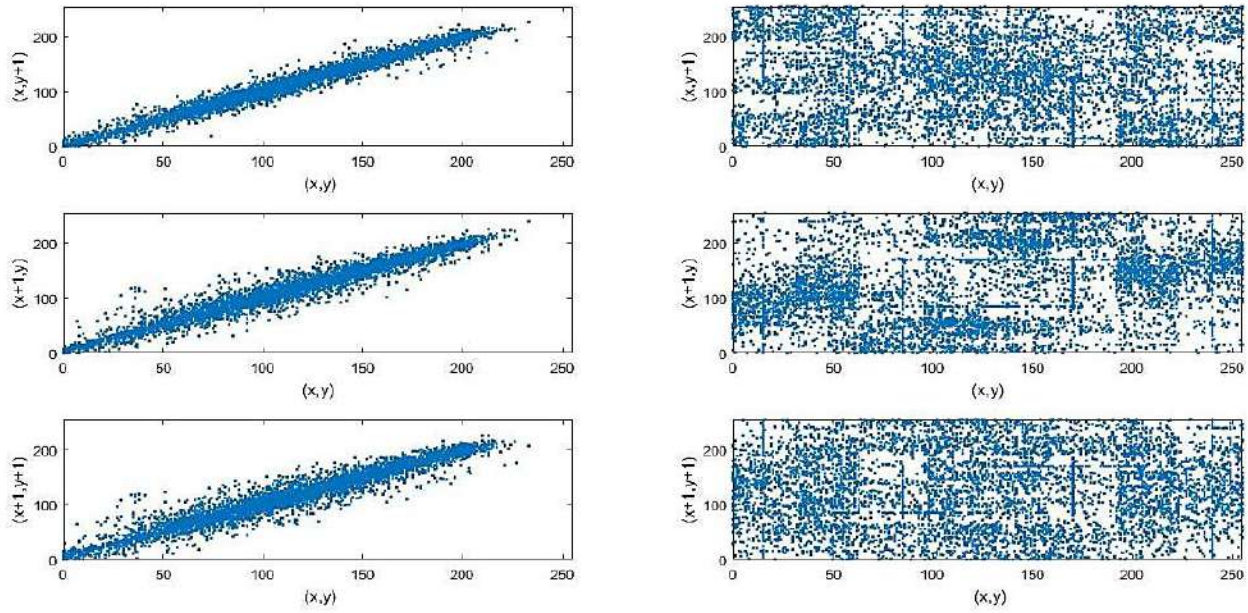


**Fig. 3.** Correlation coefficient analysis on plain and encrypted chest image

**Table 1.** Correlation coefficient, Entropy, PSNR and SSIM values for different Medical images.

| Images | Horizontal | Vertical | Diagonal | Entropy Encrypted Image | PSNR | SSIM |
|---|---|---|---|---|---|---|
| Chest | -0.1319 | 0.2975 | -0.0280 | 7.9554 | Inf | 1 |
| Mri1 | -0.8041 | 0.5730 | -0.5627 | 7.9143 | Inf | 1 |
| Mri2 | -0.5991 | 0.4760 | -0.4416 | 7.9215 | Inf | 1 |

**Table 2.** Comparison of Correlation coefficient for chest Medical image with Literature

| Images | Horizontal | Vertical | Diagonal |
|---|---|---|---|
| | | | |
| Our | -0.1319 | 0.2975 | -0.0280 |
| Ref [3] | -0.0702 | -0.0237 | 0.0023 |
| Ref [5] | -0.0679 | 0.0051 | -0.0052 |
| Ref [7] | −1.7713e-04 | 0.0015 | 0.0016 |

## V.CONCLUSION

In this work a hybrid method of medical image encryption is presented. The key method's which are utilized are DNA encoding and Affine transformation. DNA coding improves computational speed and provides large capacity for data transmission. Affine transform relocates pixels requiring intensity interpolation to approximate the value of moved pixels; also this provides bicubic interpolation which is the standard for image transformations in image processing applications. The encryption scheme is characterized by its simplicity, efficiency, and a strong level of security.Infinite PSNR, unity SSIM and negative values and even correlation distribution graph are the measures which proves the superiority of the proposed algorithm. The newly suggested approach is expected to have practical applications in various fields, including telemedicine, by enabling real-time encryption and transmission of images.

## REFERENCES

[1]. R. K. Sinha, N. San, B. Asha, S. Prasad, and S. S. Sahu, “Chaotic Image Encryption Scheme Based on Modified Arnold Cat Map and Henon Map,” in Proceedings of the 2018 International Conference on Current Trends towards Converging Technologies, ICCTCT 2018, 2018, doi: 10.1109/ICCTCT.2018.8551137.

[2].J. Ferdush, M. Begum, and M. S. Uddin, “Chaotic Lightweight Cryptosystem for Image Encryption,” Adv. Multimed., vol. 2021, 2021, doi: 10.1155/2021/5527295.

[3].S. Rohith, C. B. Sree, V. Yellapu, G. M. Basavaraj, and M. R. Mahesh, “Image Encryption Scheme Using Combined Key Sequence of Logistic and Tent Map for Medical Applications,” in 2021 IEEE International Conference on Mobile Networks and Wireless Communications, ICMNWC 2021, 2021, doi: 10.1109/ICMNWC52512.2021.9688478.

[4].P. Sreenivasulu and S. Varadharajan, “Algorithmic Analysis on Medical Image Compression Using Improved Rider Optimization Algorithm,” in Lecture Notes in Networks and Systems, vol. 103, 2020.

[5].S. Rohith, L. Jahnavi, S. C. Bhuvaneshwari, S. Supreeth, and B. K. Sujatha, “Image Encryption and Decryption Using Key Sequence of Triple Logistic Map for Medical Applications,” in Proceedings of 2020 3rd International Conference on Advances in Electronics, Computers and Communications, ICAECC 2020, 2020, doi: 10.1109/ICAECC50550.2020.9339529.

[6].W. Cao, Y. Zhou, C. L. P. Chen, and L. Xia, “Medical image encryption using edge maps,” Signal Processing, vol. 132, pp. 96–109, 2017, doi: 10.1016/j.sigpro.2016.10.003.

[7].S. Li, L. Zhao, and N. Yang, "Medical Image Encryption Based on 2D Zigzag Confusion and Dynamic Diffusion," Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/6624809.

[8].A. N. Kengnou Telem, C. Feudjio, B. Ramakrishnan, H. B. Fotsin, and K. Rajagopal, "A Simple Image Encryption Based on Binary Image Affine Transformation and Zigzag Process," Complexity, vol. 2022, 2022, doi: 10.1155/2022/3865820.

[9].K. S. Kumari and C. Nagaraju, "DNA encrypting rules with chaotic maps for medical image encryption," in Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021, 2021, doi: 10.1109/ICICCS51141.2021.9432176.

[10].P. T. Akkasaligar and S. Biradar, "Medical Image Encryption with Integrity Using DNA and Chaotic Map," in Communications in Computer and Information Science, 2019, vol. 1036, doi: 10.1007/978-981-13-9184-2_13.

[11].M. A. W. Shalaby, M. T. Saleh, and H. N. Elmahdy, "Enhanced Arnold's Cat Map-AES Encryption Technique for Medical Images," in 2nd Novel Intelligent and Leading Emerging Sciences Conference, NILES 2020, 2020, doi: 10.1109/NILES50944.2020.9257876.

[12].P. Sarosh, S. A. Parah, and G. Mohiuddin Bhat, "Fast Image Encryption Framework for Medical Images," in Proceedings of 2021 2nd International Conference on Intelligent Engineering and Management, ICIEM 2021, 2021, doi: 10.1109/ICIEM51511.2021.9445362.

[13].N. S. Goje, R. V. Ravi, D. Das, and S. S. Patra, "Biomedical Image Security Based on 2D and 3D Chaotic Systems," 3rd Int. Conf. Electron. Sustain. Commun. Syst. ICESC 2022 - Proc., no. Icesc, pp. 28–34, 2022, doi: 10.1109/ICESC54411.2022.9885677.

[14].P. T. Akkasaligar, S. Biradar, and S. Biradar, "Multilevel security for medical image using heterogeneous chaotic map and deoxyribonucleic acid sequence operations," Concurr. Comput. Pract. Exp., vol. 34, no. 24, pp. 1–21, 2022, doi: 10.1002/cpe.7222.

[15].W. S. Sayed, A. G. Radwan, H. A. H. Fahmy, and A. L. Elsedeek, "Trajectory control and image encryption using affine transformation of lorenz system," Egypt. Informatics J., vol. 22, no. 2, pp. 155–166, 2021, doi: 10.1016/j.eij.2020.07.002.